Communications of the IIMA

Volume 5 | Issue 2 Article 5

2005

War Against Spam: A Comparative Analysis Of The US And The European Legal Approach

Sylvia Mercado Kierkegaard

War Against Spam: A Comparative Analysis Of The US And The European Legal Approach

Sylvia Mercado Kierkegaard
Sylviak_1952@hotmail.com

ABSTRACT

Unsolicited commercial mail (also known as spam and junk mail) can inconvenience tens of millions of Internet users and impose huge costs on Internet Service Providers. Realizing the need to boost competitiveness and consumer confidence, the European Union (EU) and the United States have instituted various legal frameworks and policies to regulate unsolicited commercial mail. The EU has adopted an opt-in approach to spam mail, which means e-marketers need to seek the permission of consumers before they send out commercial emails, while the US CAN SPAM Act takes an opt-out approach. The EU's opt-in regime is viewed as offering greater safeguards against spam mail. Despite the EU Directive and the US federal law, the barrage of junk e-mail continues to grow. This paper discusses the issue of spam mail and makes a comparative analysis of the two legal approaches and their implications on the industry and private citizens.

Key words: Commercial e-mail, Spam, Opt-in, Opt-out, EU Directives, CAN-SPAM, fraud, harvesting.

INTRODUCTION

Electronic Mail has revolutionized the way many carry on business. It has implications for many facets of our economic and social life because it has the potential to fundamentally change the way commercial transactions, the business of government, the delivery of services and a host of other interactions are conducted, raising issues at the heart of policies directed at the regulation of traditional practices and procedures.

One of the most successful Internet marketing techniques is to include a sign-up form on their Web site to allow visitors to register for an email newsletter. The obvious temptation is to use targeted e-mail marketing. The risk here is that the advertiser may turn to a list broker and bulk-mail millions of solicitations in the hope that out of all of this a few recipients will read the message and respond. Unsolicited commercial mail (also known as spam and junk mail) can inconvenience tens of millions of Internet users and impose huge costs on Internet Service Providers. Some users see spam as a minor annoyance, while others are so overwhelmed with spam that they are forced to switch e-mail addresses. Mailing lists can be so successful, but problems develop when people cross the line from email marketing into "spamming."

Realizing the need to boost competitiveness and consumer confidence, the European Union (EU) and the United States (US) have adopted specific laws and policies to cope with the problems of spam mail and, inevitably, a minefield of accompanying uncertainties and potential pitfalls. This paper seeks to outline and compare the EU and the US efforts to regulate unsolicited commercial mail. The aim of this paper is to provide an overview of the legislations and its effectiveness. These are the areas of major importance and concern for consumers and businessmen.

SPAM

Spam is Internet slang for junk mail or unsolicited electronic mail usually sent to many people. The use of the term "spam" (a trademarked Hormel meat product) is supposedly derived from a Monty Python sketch in which Spam is included in every dish offered at a restaurant. In this skit, a group of Vikings sang a chorus of "spam, spam, spam . . ." in an increasing crescendo, drowning out other conversation. Until told to shut up (Heines, 2004). Hence, the analogy applied because spam mail was drowning out normal discourses on the Internet.

Recipients of spam often consider it to be an unwanted intrusion in their mailbox. Spam arises when a message is sent to multiple recipients, particularly for unsolicited advertising purposes. Spam mails often use spoofing. The latter is the introduction of false or inaccurate headers in emails in order to fool servers and users into thinking that

the emails came from a certain location. The danger of spoofing is that it may cause harm to an innocent network administrator when his server becomes the target of bounced emails, mail bomb attacks, and acquaintance" spam that is sent by somebody one has dealt with previously.

The first spam was sent by Gary Thuerk , a marketer for the Digital Equipment Corporation. [1] He decided to send a notice to everybody on the ARPANET which had a printed directory of everybody which they used as source for the list (Templeton, 2003). [2] The term "spam" later became popular when two lawyers from Phoenix named Canter and Siegel posted a message advertising their fairly useless services in an upcoming U.S. "green card" lottery in 1994 (OIT,2004).[3]

Technical Solutions

Technology is evolving, and many creative solutions are being introduced by Internet providers and other firms. To protect against harvesters of email addresses, some websites use software that "poisons" the harvester - for example, generating bogus email addresses or directing the harvester to a nonexistent site. Filtering the e-mail is one of the most widely used methods for managing the e-mail effectively and can prevent email-borne threats from entering the network before they can cause havoc or harm. Spam mail can be blocked by installing a mail transport agent such as *Sendmail* or *Postfix*. There are tools that bounce e-mail back to spammers, fooling them into believing the user's e-mail address is invalid with the click of a button. In the user's mail server configuration, he can bounce unwanted email messages back. *SpamCop* determines the origin of unwanted email and reports it to the relevant Internet service providers. By reporting spam, the user has a positive impact on the problem. Reporting unsolicited email also helps feed spam filtering systems.
Many spammers have become so adept at masking their tracks that they are rarely found. Spammers have adopted a new strategy by relying on malicious codes placed on consumers' machines via viruses or spyware that turn them into unwitting "zombies" remotely controlled by spammers.[4] Illegal bulk-mailers have been able to deploy massive blasts of spam by routing it through the computers of their Internet service providers, rather than sending it directly from individual machines (Krim, 2005).[5] They are so technologically sophisticated that they adjust their systems on the fly to counter special filters and other barriers thrown up against them.

Cost of Spam to Business

According to Commtouch Software, 80 percent originates from the top five spam countries, which include South Korea, (10 percent), China (6.6 percent), Brazil (3.4 percent), and Canada (3 percent.). While 49 countries have been identified as hosting Web sites referenced in spam e-mails, 56 percent of global spam e-mail originates in the U.S. (Legard, 2004). Other findings include:

- Promoting drugs is the aim of 30 percent of all spam, with Viagra alone accounting for 14.1 percent of spam.
- Spam is becoming more sophisticated in order to beat content filters, with 21.6 percent of global spam messages including visible random characters in the subject, body, or both.
- 5.8 percent of spam is written in a language other than English.

In a study released this year (2005), market research firm Rockbridge Associates and the University of Maryland Robert Smith School Of Business estimated that deleting spam alone costs nearly $22 billion a year in lost productivity (Krim, 2005).

OPT-IN AND OPT-OUT

Not all bulk email is spam. Some is permission-based, meaning that the recipient has asked to receive it. This occurs when a user at a website voluntarily agrees - for example, at the time of making a purchase - to receive email or a newsletter (known as "opt-in email"). The recipient has verifiably confirmed permission for the address to be included on the specific mailing list, by confirming the list subscription request verification. Unlike spam, opt-in email usually provides a benefit such as free information or sale prices.

Opt-out is when a company that collects information on its users through the Internet gives those users the opportunity to inform the company that it cannot use their information. This is usually a check box beneath the form where the user fills out the information. Some businesses, however, have misused the practice of opt-out. They give customers the opportunity to opt-out, but the problem is that they go to great lengths to hide that check box or force the user to jump through hoop after hoop. The reality is that these disclaimers will likely be buried in lengthy, small print, legalistically worded, privacy policies a link or two away from the sign up form itself. And of course few users

will read policies that were designed specifically not to be read. So the fact of permission will be achieved, but not the spirit.

THE EU APPROACH

Recognizing the problem that spam/unsolicited commercial mails generate, the EU has issued five directives, which are relevant in regulating spam.

- Data Protection Directive 95/46
- Distance Selling Directive 97/7/EC
- Electronic Commerce Directive 2000/31/EC
- Directive 2002/58/EC

The Data Protection Directive

Directive 95/46 establishes a property right in personal data, by which the data subject may exercise certain exclusionary rights against the collection and processing of data. E-mail address is a form of personal data, as defined in Article 2(a), because it is capable of relating to an identified or identifiable human data subject. Article 7 states that "information may be processed only when the data subject has given his consent unambiguously except when those interests are outweighed by the individual's interests." It will not be enough to provide a small opt-out box in an inaccessible corner or a hyper-link to an opt-out page to satisfy the consent requirement. [6]

Of importance to direct marketing is Article 14 (b), which provides data subject the right to object and prohibit one's e-mail address from being collected and subsequently used for the purpose of spamming by the controller or some third party. It provides two alternative approaches for giving the data subject the right to object. The first does not require specific action by the controller, although Member States are charged with the duty of taking necessary measures to make data subjects aware of their rights to object free of charge the processing of their personal data for marketing purposes. Therefore, the controller does not need to inform the data subject if his awareness of the existence of the right has been achieved by appropriate measure such as publicity. The second approach requires the data subjects are expressly offered the right to object before the data are used or disclosed for the first time for direct marketing purposes.

The Directive is silent on whether a once and for all assent will suffice or whether the data subject should be asked periodically. Factors to consider in choosing which alternative would suffice would be to take into account whether the controller would be reusing the data for new uses, which the data subject has not agreed to.

Distance Selling Directive

Article 10 of Directive 97/7/EC on the Protection of Consumers in respect of Distance Contracts and Directive 2002/65/EC on distance marketing of financial service restrict the use of certain means of distance communication without prior consent. In Annex 1, the means of distance communication referred to in Article 2 (4) includes electronic e-mail. Therefore the consumer can object and prohibit, in the context of distance selling, from his e-mail address being distributed for the purpose of spamming.

Directive on Ecommerce

Directive 2000/31/EC covers several crucial aspects in the relationship between electronic commerce and advertising. A definition of commercial communications, the clarification of the information that will have to be provided by service providers and a series of dispositions dealing with the growing problematic of "junk mail" or unsolicited commercial communications are the main pillars of the directive in advertising-related matters. The Directive takes a slightly different approach regarding spam. It allows member states to enact law permitting unsolicited commercial emails, provided that the sender is clearly and unambiguously identifiable [Art.7 (1)]. However, Article 7(2) mentions neither the possibility of Member States prohibiting unsolicited commercial communications nor the possibility of Member States imposing a requirement of the recipient's prior consent for the sending of such messages.

The Directive has some shortcomings. Although, the sender's identity has to be clearly stated, it does not necessarily mean that the spammer is obliged to act upon requests for removal from a mailing list. Also, the identification process does not necessarily mean that the request for removal process is costless. A spammer who provides a phone number for the request for removal process may charge a high free for such removal. The Directive requires

spammers to regularly consult and respect the opt-out register provided by service providers [Art.7 (2]. By thus confining itself to laying down an obligation of regular consultation of opt-out registers, the Directive promotes a technical measure the only purpose of which is to implement an opt-out approach. [7] However, it does not indicate how an opt-out register is to be constructed, i.e. whether it is a single register for the whole EU or a multiple industry-register, nor does it require the opt-out registers to be systematically consulted prior to the sending of any message, but merely that they will be consulted "regularly". However, the term "regular" consultation is ambiguous as it does not mean prior or systematic consultation.

Privacy Directive

In order to resolve the ambiguity of the EU legislations on spam mails, and to complement the existing Data Protection Directive, the EU adopted the Directive on Privacy and Electronic Communications 2002/58/EC. It regulates privacy and data protection issues as a result of new online marketing practices in B2C transactions. The most important provision concerning unsolicited communication is contained in Article 13 which provides that the use of automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail for the purposes of direct marketing may only be allowed in respect of subscribers who have given their prior consent. [8]

The opt-in approach is softened somewhat by a provision, which allows companies to target customers who have bought products or services from them in the past. This is, however, subject to a number of provisos: Firstly, the customer's details must have been collected in the context of a "sale" - on a strict interpretation, this could rule out the use of contact details of potential customers who have merely registered an interest in a service or product. Just how much scope there is to lobby the individual governments for a flexible approach on this issue remains to be seen. Secondly, the customer must have been told about the possible use of his or her data for future marketing at the time it was collected - i.e. at the time of the initial purchase - and given the chance to object. The opportunity to opt-out must then be given with each subsequent marketing message. Thirdly, the customer's details may only be used by the same entity to which they were given originally. This clearly has implications for transfers of customer lists between group companies and trading partners. Finally, these provisions would be subject to a further requirement that the marketing be for a "similar product" to that in relation to which the customer's details were originally gathered. This will undoubtedly lead to uncertainty for businesses about just how "similar" the new product advertised needs to be to avoid breaching the legislation.

The practice of disguising or concealing the identity of the sender of unsolicited communications, or failing to provide an address to request that such communications cease is also prohibited. The "opt-in" requirement is designed to cover both current methods of transmitting messages as well as future methods, as technology develops.[9]

The opt-in principle required by this Directive solves one of the hardest questions of what is consent. It is particularly important because under Directive 95/46, the data subject's consent "shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed." This could be interpreted as either opt-in or opt-out. In other words requiring customers to indicate if they do not want to receive unsolicited mail is no longer good enough. This has a major implication for the way forms and notices in electronic form are handled. Individuals should now opt-in to their data being used in other ways, rather than opting out as was the case.

US APPROACH

The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act 2003) covers all commercial email, not just unsolicited e-mail, but it does not seem to address non-profit and personal email. The one notable exception to applicability of most provisions of the Act lies in emails of a "transactional or relationship" nature [Sec3 (17)]. [10]

In §3(2), the bill defines commercial electronic mail message as: any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service including content on an Internet website operated for a commercial purpose. [11]
An integral provision of the Act is its pre-emption of any state law that "expressly regulates the use of electronic mail to send commercial messages, except to the extent that any such statute, regulation or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto." However, the

Act does not pre-empt state laws that are not specific to electronic mail, including common law causes of action and laws that "relate to acts of fraud or computer crime" [Sec.8 (b)].
The law requires that all e-mail – including business-to-consumer and business to-business for which the primary purpose is the advertisement or promotion of a commercial product or service to include the following:

- Prohibition of false and misleading information. Specific prohibited practices include falsification of header information, hijacking another e-mail server to send or relay spam, false registrations for email accounts or IP addresses used in connection with email ads in order to hide one's identity, and retransmissions of email ads for the purpose of concealing their origins;
- Prohibition of deceptive subject headings;
- Inclusion of functioning return electronic mail address or other comparable Internet mechanism which should be clearly and conspicuously displayed or e-mail unsubscribe system that operates for at least 30 days after the original message is sent [Sec. 5(3)]. In addition, it must include the postal address and a clear indication that the e-mail includes a solicitation, unless the senders have "prior affirmative assent" from the recipient [Sec. 5(a) (5)].
- Clear and conspicuous notice of the opportunity to decline to receive further commercial e-mail messages from the sender. The Act permits the mailing of email ads to persons who have not agreed to receive them and who have no pre-existing or current business relationship with the sender. However, the sender of such emails must give the recipient the ability to send a reply message or other "Internet-based communication" that opts out of future emails from the sender.
- Prohibition of commercial electronic mail after objection. The sender of the message may not send subsequent advertisements or promotions more than 10 business days after the request from any recipient to be removed from future commercial e-mail communications. [12]
- Prohibits Address Harvesting and Dictionary Attacks; [13]
- Prohibits the automated creation of multiple e-mail accounts to transmit otherwise unlawful messages and the relay or retransmission of commercial email from computers that have been accessed without authorization;
- Requirement to place a) warning labels on commercial electronic email containing sexually-oriented materials which include in subject heading initially viewable specific marks or notices to ensure that when the message is opened, it includes only the mark or notice indicating that the message is sexually oriented b) prior affirmative consent c) Instructions on how to access the sexually oriented material;
- The law also will make it unlawful for a business to promote goods and services in a commercial e-mail message sent by others which the business knows violate provisions of the law. Thus, it implicates not only spammers, but those who procure their services.

Sounds tough, but the proof is in the pudding. A year after the CAN-SPAM Act kicked off, 97 percent of unsolicited commercial email failed to reduce e-mail clutter, the problem continues to grow and the anti-spam law has so far proved useless (Wakefield, 2005). An array of research shows that purveyors of spam have done little to change their behaviour. Spam could be costing an average company $4.1 million a year in lost productivity, according to IDC (Koptoff, 2004). Unfortunately, the Act attempts to regulate rather than ban the practice of spamming.

According to Spamhaus (2005), by letting the industry know that spam was legal in some form in the United States, is inviting a tsunami of spam from Asia. By requiring that American citizens read through and respond to every spam to 'opt out' of ever-more mailings they did not opt in to, millions will find their addresses sold on as 'people who read spam's" and will find themselves endlessly on yet more lists.

The opt-out rule is ineffective because there is no legal compulsion to provide individuals with an obvious opt-out link. It simply requires that an "Internet-based mechanism" must be provided. The opt-out link could be so inconspicuous that individuals it will be virtually impossible to find it or so complicated that it might take hours to unsubscribe. In addition, by allowing the companies to spam for 10 more days after one has opted out, it is more of a of a 'U-CAN-SPAM' Act.

CAN-SPAM also contradicts many statewide laws across the US that prohibit the practice of sending non-fraudulent spam. Washington State, for example, has granted individuals the right to sue spammers, while California and Delaware have mandated an opt-in approach similar to that now enforced in the EU.

COMPARATIVE ANALYSIS

The CAN-SPAM Act allows companies to send email ads to potential customers, even where the recipients have not given prior consent to such mailings and even where the sender does not have a pre-existing or current business relationship with the recipient. The US takes an opt-out approach, meaning that each spammer can e-mail the recipient until the latter asks them to stop, and allows the spammer to dictate what steps individuals must take to get off their list. [14] The burden for avoiding unwanted commercial email falls on the individual to unsubscribe, rather than providing effective constraints to prevent marketers from sending unwanted email. The spammer can also force the recipient to opt-out via a list or menu from which the recipient may choose the specific types of commercial electronic-mail messages the recipient wants to receive or does not want to receive from the sender" just as along as opting out from all e-mail from that sender is one of the choices". Thus, the US approach is much less strict than the 'opt-in' approach adopted by EU legislation which is viewed as offering greater safeguards against spam.

Unsolicited commercial electronic mail and affirmative consent are defined too imprecisely to effectively regulate spam. In section §3(1), the bill defines affirmative consent as :" (A) the recipient expressly consented to receive the message, either in response to a clear and conspicuous request for such consent or at the recipient's own initiative; and (B) if the message is from a party other than the party to which the recipient communicated such consent, the recipient was given clear and conspicuous notice at the time the consent was communicated that the recipient's electronic mail address could be transferred to such other party for the purpose of initiating commercial electronic mail messages." The sender is not prevented from selling their lists of addresses, so long as the recipients were given "clear and conspicuous notice" that their addresses would be released to a third party. Then, the affected individual email users will have to opt-out of email from every sender.

One of the CAN-SPAM Act's surprising features is its failure to create a broad exemption for emails sent to recipients with whom the sender has a pre-existing or current business relationship. Such an exemption, which is common in state anti-spam laws, permits businesses to contact their past and present customers without observing all of the restrictions that apply to emails sent to strangers. Instead of creating a pre-existing or current business relationship exemption, the new Act recognizes only a narrow category of "transactional" or relationship messages. In contrast, the EU Directive provides exceptions to the opt-in rule to businesses which have already obtained the person's contact details in the context of the sale of a product or service. Marketing activities directed at those persons could then take place only if they relate to similar products or services and if customers are given the opportunity to unsubscribe free of charge in an easy manner. So far, the Member States' interpretation of this provision has differed significantly, leading to confusion over what practices are tolerated. Indeed, varying degrees of protection were granted to businesses across the EU which made complying with the directive an uneasy task. Critics also argue that what is considered spam in the EU won't be considered so across the pond and spammers can use this fact to their advantage.

The CAN-SPAM Act does not permit recipients of commercial emails to sue the senders for violations of the Act (Sec.7).Enforcement will be primarily by means of actions brought by the FTC or state law enforcement authorities. Internet service providers, however, have a right to bring civil lawsuits against violators that adversely affect those providers. In contrast Directive 95/46/EC (Arts.22 and 23) requires Member States to provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question. Firms that continue to send spam face hefty fines and, in certain circumstances, can be sued by the recipients.

IS THE LAW WORKING?

Despite the EU Directive and the US federal law, the barrage of junk e-mail continues to grow. According to Email Systems, Florida is the spam capital of the world (Barkham, 2005). Anti-spam lobby group Spamhaus (2004) said that 90% of Europe's spam problem originates in the United States. It estimates that by the summer of 2006, spam will account for 95% of all e-mails sent and the problem will not be alleviated until the US acts to toughen its laws. It also claims that only 200 spam operators are responsible for 80 percent of the spam received by Internet users in North America and Europe and it is well-known exactly who these "spam kingpins" are. Shutting these operators down, then, should drastically reduce the spam clogging our inboxes (Ramasastry, 2004).

There have been some prosecutions and lawsuits, but not nearly enough mainly because the law forbids individual Internet users from suing junk e-mailers. When it comes to prosecuting spammers, authorities have to apply local state laws, instead. For example, Jeremy Jaynes got nine years in jail under the Virginia's antispam law for sending ten million junk e-mails each day and a $7,500 fine for his sister. Unfortunately, their conviction was overturned in

March 2005 when the judge ruled that that the jury had been misled by the case's technological terms and the anti-spam law used to convict the pair had confused the jurors (Webhost Industry Review, 2005). Apparently, the family that spams together won't get sent to the can together.

Although a $1.08 billion judgment by Judge Charles Wolle to Robert Kramer, owner of CIS Internet Services, an ISP based in Iowa against three US spammers has been hailed as a huge success in the war against unsolicited email (Gross, 2004), the fight against spam set a judicial set-back when U.S. District Judge Alvin Hellerstein federal judge refused to accept a guilty plea from a former America Online employee accused of selling the Internet provider's customer list to a "spammer," saying he was unsure a crime had been committed .At issue", the judge said," is whether the actions rose to the level required by a new anti-spam law, which states that spam must be not only annoying but deceptive" (Hu, 2004).

In contrast, many countries from Western Europe have been vigilant in prosecuting spammers. Dutch authorities have issued their first fines for spam originating in the country. Telecommunications regulator OPTA, which is responsible for regulating spam in the Netherlands, issued three separate fines in January of 2004, the first since the Dutch government agreed in 2004 to a ban spam mails (Blau, 2004). In an another case, the Netherlands Supreme Court ruled that Internet provider XS4ALL is permitted to refuse spam on its network. This marks the end of a legal case brought by XS4ALL at the beginning of 2002 against the spammer AbFab. [15]

In Denmark, the court handed down a 400,000 Kroner fine after the company - Aircom Erhverv - was found guilty of sending 15,000 unsolicited commercial faxes (Richardson,2004). The latest spammer to fall foul of Danish law is a businessman who has been convicted of sending out more than 10,000 spam emails. While Denmark has been on spammers' cases for some time, the rest of the EU is not faring so well. Some of the Member States have yet to implement the directive, prompting the European Commission to start legal action against them (Dunn, 2004).[16]

CONCLUSION

Even with the anti-spam legislation, the future of spamless email looks beak. The e-mails that were the root of the problem are still as omnipresent as ever. Although the CAN SPAM Act regulates the manner of spamming, it will only have a deterrent effect on the vast majority of spammers who care little about the law. Arrests have been made, fines handed out and even jail time awaits some spammers, but yet, the bombardment of junk continues. Spammers simply move their operations offshore to countries where the laws are less troublesome. The US and the EU simply cannot stop spam which originates in the US and countries outside their border. Arresting or prosecuting numerous spammers is like using a sponge to soak up a sidewalk puddle during a rainstorm.
There is no silver bullet to stop spam or spammers. If a business relies on legislation to handle the spam problem, they are pretty much out of luck, unless the US moves quickly to toughen its laws. The best anti-spam solutions may well be technologically-based. Businesses in the US and Europe could prevent the spam mails from arriving in inboxes by using spam filters. Unfortunately while technical solutions are crucial, it will not catch all spam. Technology, even with constantly improving filtering software, is not likely to eliminate spam on its own. [17]

Without international cooperation requiring countries to impose an "opt-in" system, legislations are powerless to stop spam mails coming from countries like China or Russia, or hijack so-called zombie PCs from any country in the world in order to send their spam messages. [18]A Council on Internet Communications has just been formed and its aim is to coordinate international efforts to stop spammers. This sort of international group is necessary because spammers operate internationally. The extent to which spam is eventually limited or controlled will be, in large part, defined by international cooperation between ISPs, consumers, online communities, and government enforcement agencies.

REFERENCES

Blau, J.(2004, December 29).Netherlands issues first fines to Spammers. The Industry Standard. Retrieved 30 June, 2005, from http://www.thestandard.com/internetnews/2004_12.php

Dunn, J. (2004, April 28). EUs Anti-Spam Laws in Chaos. Techworld. Retrieved 30 June 2005,from http://www.thestandard.com/article.php?story=20040428163130208

Gross, G. (2004, December 21).Judge Awards ISP US $1B in Damages. IDG News Service. Retrieved 30 June, 2005, from, http://www.infoworld.com/

Heines,L.(2004, June 17) Spam King Ritcher Gets Legal Roasting. The Register. Retrieved 30 June 2005, from http://www.theregister.co.uk/2004/06/17/spam_king_roasting/

Hu, J. (2004, December 21). Judge Denies Guilty Plea in AOL spam case. CNet Networks. Retrieved 30 June, 2005, from, http://news.com.com/

Kopytoff, V. (2004, September 2).Spam Mushrooms. San Francisco Chronicle. Retrieved 30 June 2005, from, http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2004/09/02/BUGVJ8I4AS1.DTL

Krim, J. (2005).Spammers New Strategy. Washington Post.

Leyden, J. (2003, November 24).US anti-spam edges towards law. The Registrar. Retrieved 30 June 2005, from, http://www.theregister.co.uk/2003/11/24/us_antispam_bill_edges_towards/

Legard. D. (2004, July 5). Amount of Spam still skyrocketing. IDG News Service. Retrieved 30 June 2005, from, http://www.pcworld.com/news/article/0,aid,116785,tfg,tfg,00.asp

Privacy and data protection. (2004). Info Society. Retrieved 30 June 2005, from http://www.euractiv.com /Article?tcmuri=tcm%3A29-117532-16&type=LinksDossier

Ramasastry, A. (2004, December 15). In Virginia, Ohio and Maryland, Kingpin Spammers Go to the Slammer. FindLaws Legal Commentary. Retrieved 30 June 2005, from, http://writ.news.findlaw.com /ramasastry/20041215.html

Richardson, T.(2004,January 21).Danish Spammer Fined 37K.The Register. Retrieved 30 June 2005, from, http://www.theregister.co.uk/2004/01/21/danish_spammer_fined_163_37k/

Spam. (2004). Office of Information Technology. Retrieved 3 March, 2005, from, http://www.ocean.edu/campus/oit/SpamArticle/SpamArticle.html

The Spamhaus project news . Available at : http://www.spamhaus.org/newsindex.lasso

Spam and the Internet. (2005). Retrieved on 8 March 2005, from http://www.spam.com/ci/ci_in.htm

Templeton, B. (2003). Reflections on the 25th Anniversary of Spam. NPR. Retrieved 30 June 2005, from, http://www.templetons.com/brad/spam/spam25.html

Spam Conviction Overturned. (2005, March 4). Webhost Industry Review. Retrieved 30 June 2005 from, http://thewhir.com/marketwatch/spa030405.cfm

XS4ALL wins appeal in cassation in spam case.(2004).Retrieved 2 June 2005 from:http://www.xs4all.nl/uk/news/ overview/abfabhr.html

CAN-SPAM Act of 2003. Available at http://www.spamlaws.com/

EU Legislations available at: http://europa.eu.int/

ENDNOTES

[1] It was the leading minicomputer maker, and its computers provided the platform for the development of UNIX, C and much of the internet. In 1978, the Arpanet (now known as the Internet) had already provided network E-mail to a large number of folks at universities, government institutions and universities for over 6 years.

[2] The term goes back to the late 1980s and was applied to a few different behaviours. One was to flood the computer with too much data to crash it. Another was to "spam the database" by having a program create a huge number of objects, rather then creating them by hand. The term was sometimes used to mean simply flooding a chat session with a bunch of text inserted by a program.

[3] It was the first deliberate mass posting to commonly get that name. They had posted their message to every single newsgroup (message board) on USENET, the world's largest online conferencing system. There were several thousand such newsgroups, and each one got the ad.

[4] The use of multiple zombies on the networks of large Internet service providers allows spammers to spread out the amount of mail sent by any one computer, helping them to fly under the radar of ISP limits. That and other tactics have allowed spammers to circumvent many technical measures taken by network operators to thwart them, and they have all but ignored laws that prohibit their activities.

[5] The result is that "blacklists" of known spamming computers - which other network operators rely upon to block mail from those machines - are no longer effective. To block spam coming directly from an ISP's computers, all mail from that ISP would be have to be blocked, which would cripple electronic communication.

[6] In the UK case of *Linguaphone Institute v Data Protection Registrar(*C-DA/94/49/1*)* the plaintiff used a small opt-out box in the bottom corner of advertisements. In the Tribunal's view the position, size of print and wording of the opt-out box does not amount to a sufficient indication that the company intends or may wish to hold, use or disclose that personal data provided at the time of enquiry for the purpose of trading in personal data.

[7] Prior to the adoption of Directive 2000/31/EC, the right to opt out could apply only in respect of a relationship between a particular individual and a particular service provider. However, Directive 2000/31/EC introduces a right to opt out from receiving commercial e-mails from all service providers established in Europe, without requiring that the collecting party or the third party advertiser be informed as to the exercise of the right of objection..

[8] As a consequence, any form of interception or storage of private communications is to be prohibited without the users' prior consent ('opt-in' system) - the user being identified as a private individual or a business

[9] Companies operating in the EU have to obtain the consent of mobile phone users before sending commercial messages via SMS (Recital 40).

[10] This narrow exception applies to emails regarding, in part: messages sent to complete a transaction or sale or deliver goods or services; Warranty, product updates, upgrades, or recall information; Safety or security information about a product used or purchased by recipient; Change in terms or features of a subscription or service; information about employment relationship or related benefit plan; and deliver of goods and services, including product updates and upgrades [Sec3 (17)].

[11] However "inclusion of a reference to a commercial entity or a link to the website of a commercial entity in an electronic mail message does not, by itself, cause such message to be treated as a commercial electronic mail message if the contents or circumstances of the message indicate a primary purpose other than commercial advertisement or promotion of a commercial product or service."

[12] If the recipient has requested not to receive further advertisements or promotions, the sender may not request, sell, lease, exchange, or otherwise transfer or releases the email address of the recipient.

[13] Harvesting is the practice of collecting, through an automated means, e-mail addresses that are posted on websites or online services. Dictionary attacks occur when e-mail addresses are generated by combining names, letters, or numbers into numerous permutations in the hope of generating functioning email addresses.

[14] The recipient must opt-out "in a manner specified in the message" that can include replying to an opt-out email address or "other Internet-based mechanism."

[15] The Supreme Court stated :"*Anyone who without authorisation makes use of property to which another party has an exclusive right, and who thereby infringes that exclusive right, is acting unlawfully vis-à-vis the beneficiary of the right, unless there is justification. The right to freedom of speech does not constitute such justification. This fundamental right cannot serve in principle to justify transgressive use of property to which another party has exclusive rights* (http://www.xs4all.nl/uk/news/overview/abfabhr.html).

[16] A study by the Institute of Information Law at the University of Amsterdam has revealed that the EU's much-vaunted anti-spam legislation, Directive 2002/58, which was supposed to have been adopted by member states by October 2003, have only been implemented into national legislation by 7 of the then 15 members by the cut-off date and countries that have implemented the Directive were attaching widely varying penalties for offenders ranging from fines to imprisonment

[17] Spam scams are becoming ever more sophisticated. "Phishing" is the new buzzword in internet crime. Automatically generated emails cleverly copy real corporations, fooling users into disclosing personal information - and credit card details - to criminals, who then empty their bank accounts. Many Internet Service Providers based in the United States have not improved their anti-spam enforcement.

[18] Zombies are PCs that have been compromised by hackers or virus writers.